



Guidance for Using Wireless Two-Finger Identification Devices (RapID)

**A Fact Sheet Prepared by the Kansas Bureau of Investigation (KBI)
October 2008**

What is a wireless two-finger identification device (RapID)?

A wireless two-finger identification device, commonly referred to as a RapID, is a handheld instrument used to take digital fingerprints. This instrument can be used to identify a suspect while in the field without having to return to the station. Once scanned, the fingerprints are transmitted via cellular phone to the KBI Automated Fingerprint Identification System (AFIS) database to search for matches.

How is identity established once the fingerprints are transmitted?

Fingerprints are compared with all fingerprints held in the state of Kansas central repository, which is operated by the KBI and located in Topeka, Kansas.

Does the RapID search against the national fingerprint database at the Federal Bureau of Investigation (FBI)?

No, the national database is not searched. Currently the FBI does not have the capability to receive and compare prints from a wireless two-finger identification device. However, the FBI is working to provide this functionality in the future.

How long does it take to receive search results?

Officers should receive search results in less than three minutes. However, this may vary depending on such factors as the volume of fingerprint traffic being processed by the central repository and the quality of the wireless connection available to the RapID.

When can a law enforcement officer use the RapID?

The RapID device can be utilized when an officer has reasonable suspicion that a person is, or has been, involved in criminal activity. The officer must reasonably believe that determining identity will establish or negate that person's involvement with the criminal activity. Such

circumstances are commonly referred to as “Terry stops.” See *Terry v. Ohio*, 392 U.S. 1, 88 S.Ct. 1868 (1968).

Does an officer’s request for identification constitute a Fourth Amendment seizure?

No. When an officer has reasonable suspicion that a person may be involved in criminal activity, the officer may stop the person briefly and investigate further.

Does a suspect have to consent to being fingerprinted by a RapID?

Although consent is best, it is not necessarily required as long as the officer has reasonable suspicion that a person is, or has been, involved in criminal activity, and reasonably believes that determining identity will establish or negate a person’s involvement with such activity.

How long can a suspect be detained for the purpose of utilizing the RapID and taking fingerprints?

The detention must be limited in scope, purpose and duration, and must last no longer than necessary to carry out the purpose of the stop. In addition, the investigative methods should be the least intrusive means reasonably available to verify or dispel the officer’s suspicion in a short period of time.

Under what circumstances should a law enforcement officer not use RapID?

If an officer has no reasonable suspicion that a person is, or has been, involved in criminal activity, the officer should not utilize the RapID. An officer may approach an individual on the street for investigative purposes, ask the individual’s name and request identification. However, an officer cannot force the individual to answer and the individual is free to leave at any time. In such situations, use of the RapID is not justified.

How long are fingerprints retained?

They are not retained in the database. After the identification process is complete and the response message is sent to the submitting RapID, the central repository system purges the fingerprints submitted by the RapID.

Where can I obtain more information regarding legal aspects of using the RapID?

Contact legal counsel for your agency to obtain further information.